

OVERVIEW

Mobile technology allows Michigan Department of Health and Human Services (MDHHS) staff to have remote access to the State of Michigan (SOM) network and allows staff to perform their work duties outside of the office. Mobile technology includes computers and Virtual Private Network (VPN) access.

POLICY

Remote access is for use by state employees and contractors that require access to State of Michigan applications, files and networks to perform State of Michigan business.

If mobile technology equipment is lost, stolen or damaged due to employee negligence, the employee may be subject to corrective and disciplinary action and/or restitution; see APT 301, Mobile Worker Equipment Accountability.

Note: Staff may not use personal devices to access MDHHS data.

PROCEDURE

A request for a VPN must be sent by the manager or the designated IT liaison not individual users. The A supervisor or division director must approve requests for VPN based on MDHHS operational need. To request, update, renew or cancel remote access and VPN tokens, complete a [DTMB-0051, Remote Access Request](#).

1. From [MILogin for Workers](#)/Request Access, complete a *Search Application* for VPN then click on MDHHS OBRA (SOM Intranet or VPN Only).
2. Agree to the terms and conditions and then click **Request Access**.
3. Complete additional information requested and click **Submit**.

Note: For more information see the Michigan Department of Management and Budget (DTMB) website [Remote Access and VPN Tokens](#).

4. An authorized approver must approve the request for remote access.

CONFIDENTIALITY

Records of MDHHS contain confidential information and employees must maintain the confidentiality of these records. Staff who inappropriately release confidential information subject themselves to potential criminal penalties, fines and costs. Employees who intentionally or unintentionally violate confidentiality requirements may also subject themselves to personal liability and corrective and disciplinary action. MDHHS may also be civilly liable. See:

- Services Requirements Manual ([SRM](#)) [131, Confidentiality](#), for confidentiality policy and procedures for children's protective services (CPS), foster care (FC), adoption (ADOPT), juvenile justice (JJ), and references to prevention and adult services.
- Bridges Administrative Manual ([BAM](#)) [310, Confidentiality and Public Access to Case Records](#), for confidentiality policy and procedures for financial assistance programs.
- Administrative Policy Manual Hospitals and Facilities ([APF](#)) [142, Disclosure of Confidential or Privileged Information](#), for disclosure for recipients of mental health services.
- Administrative Policy Legal ([APL](#)) [General Policy for Compliance with HIPSS Regulations](#), to assure confidential information is treated in accordance with federal and state law.

REFERENCES

[Fraudulent Access to Computers, Computer Systems, and Computer Networks Act](#) (MCL 752.791 et seq.)

CONTACT

For more information contact Bureau of IT Support Services, IT Asset Management.